International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 4, May-June 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Image to Image Encoder using Least Significant Bit

Samthomas Raphael[1], Dr. Ganesh D[2]

[1]Master of Computer Application, [2]Associate Professor,
[1,2]Jain Deemed-to-be University, Bengaluru, Karnataka, India

ABSTRACT

The purpose of "Image to Image Encoder" is to hide an image inside another image. Using the LSB method, which facilitates data hiding in an image. It works with JPEG and PNG formats for the cover image and always creates tiff encoded image due to its compression. Least Significant Bit Embeddings (LSB) are the general steganographic procedure that might be utilized to install information into a variety of digital media, the most studied applications are utilizing LSB embedding to hide one picture inside another. The security to keep up secrecy of message is accomplished by making it infeasible for a third individual to distinguish and recover the secret message.

This method can be used in various fields for data security like for secret communication and data transfer via networks, for storing and transferring sensitive data and information in the defense sector. As the normal viewers can not identify the slight difference in the encoded image without the reference of the original cover image, this method ensures more security than cryptographic methods.

KEYWORDS: *Digital Image, Secret Image, Cover, Steganography, Encoding, Decoding, Data Security*

How to cite this paper: Samthomas Raphael | Dr. Ganesh D "Image to Image Encoder using Least Significant Bit" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-4, June 2021, pp.369-372, URL: www.ijtsrd.com/papers/ijtsrd41253.pdf

IJTSRD41253

INTRODUCTION

Data security has developed as a major issue in our advanced life. The advancement of new transmission methods powers a particular strategy of safety mechanisms particularly in state of the communication of data or information. As the size of data transmission across internet increases, the significance of information security also increases. When these transferred data are valuable or confidential, intruders or attackers try to expose, alter or destroy it or use it for more difficult attacks. This is where the importance of data protection arises. There are several techniques used for ensuring personal or private communication of data. While talking about data, images take a lion's share in the data that is shared through the internet. Most of the times these images are of great importance to the people who send or receive it. It can be personal photographs, confidental images etc. This is in the case of normal people. When it comes to the data communication between organisations or governments or agencies related to them, these images might be of much more importance that can cause dangerous threats when it falls on intruders hands. So its crucial to prevent or avoid attacks or actions to access these data while transferring them. This project uses steganographic techniques to hide an image inside another image so that the image inside the cover image will be safe from the attackers eyes. These encoded images can be transferred through internet without the fear of data thefts since the attackers are unaware of the secret image inside it.

METHODOLOGIES

A. Least Significant Bit (LSB) Algorithm

The well-known strategy used for steganography is the Least Significant Bit. And additionally the prominent technique for the present day, steganography is to utilize LSB of picture's pixel data. This investigation is utilized for one piece of the LSB. It inserts each piece of the double content piece with one piece of every pixel in the first picture. This strategy works when the record is longer than the message document and if picture is grayscale, when applying LSB strategies to every byte of a 24 bit picture, three bits can be encoded into every pixel. Example: We can hide data in images by replacing the last bit of every color's byte with a bit from the secret image.

B. Existing System

There are several encoding techniques that are often used in day-today functions to ensure data security. Most of them are using cryptographic techniques. But when using cryptography, the data is visible or available to trespassers who see the data or intruders who tries to access the protected data even though it is in the encrypted format. If they have the right tools to decrypt it, they can break the security easily and decrypt and fetch the protected data. It means that one way or another, an intruder can figure out the presence of the hidden data which results in the compromise of sensitive data.

C. Proposed System

In this method, we are using steganographic technique instead of cryptography. In this method, the intruders or trespassers cannot know about the presence of the image which is hidden inside the cover image. Without a reference of the original cover image it is impossible to find the presence of the secret image inside the encoded image. So this method ensures more data security to the users in data hiding for storage and transfer.

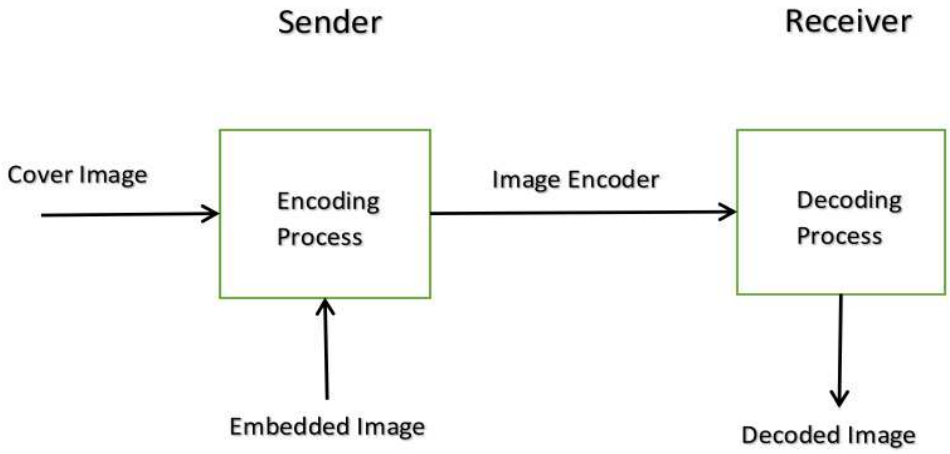

Figure 1: General Process Diagram

D. Steganography vs Cryptography

Cryptography is the method used for the conversion of the data into encrypted format by using the symmetric key and this process is known as the encryption. The primary drawback of the cryptography approach is that the encrypted data is visible but we can't read it. Steganography is the method for data embedding where the data to be kept secret is concealed into the digital media .In this process the Trespasser can't be able to see the plaintext or the cipher text because it is concealing into the another media. The trespasser can't suspect if thereis any confidential data that is existing. The steganography technique is used for the better security of the data over the computer networks.

E. Process

An image is represented as a set of pixels and each pixel in an image is represented by a coordinate (x, y) with a color, and these colors are represented with a tuple with the intensity of three RGB colors (red, green, blue). Each of these RGB colors goes from the range of 0 to 255 and we can represent that number as a 8 digit binary number, for example, 192_{10} = 1100 0000_{2}19210=110000002. Now, the most significant bits in that number are 11001100 and the rest (00000000) does not contribute that much value to the information, so these bits are called least significant bits .

Let's consider Pillow. Pillow is a friendly fork of of Python Imaging Library, it is very effortless to use and it supports many image file formats and operations. This can be extended to support even diffrent file formats. Using Pillow as a virtual canvas to draw using pixels is easy. An existing image can be read and get not only image but information regarding pixels also. In this case we want to conceal that secret image inside the covering image. Here is the idea of LSB and MSB comes in to application. The concept is extracting the MSB from the image to hide and replace it with the Least Significant Bit of the cover up image. At the end we should generate an image almost identical to the cover but hiding the secret image.

As mentioned before, the idea is very simple, we take the image we want to hide and read the color channel information for a given pixel, let's say, pixel (312, 216) has color information (53, 31, 109). Now, we read the same color info from the image we will use as cover up, (181, 200, 220). Then comes the most important and interesting part, we take the color info one by one, convert them into binary, 181_{10} = 1011 0101_218110=101101012 for the cover image pixel of the red channel (312, 216) and 53_{10} = 0011 0101_25310=001101012 for the pixel in the same embedding image, and we take 4 bytes most significant bits from the embedding image and place them instead of the 4 bytes least significant bits of the covering image (cover up), resulting 1011 0011_2 = 179_{10}101100112=17910 for the same pixel, notice even in decimal there is no much distance or difference between the original color channel for red (181_{10}18110) and the resulting secret (179_{10}17910), we repeatedly perform this process for every pixel of the image and color channel.

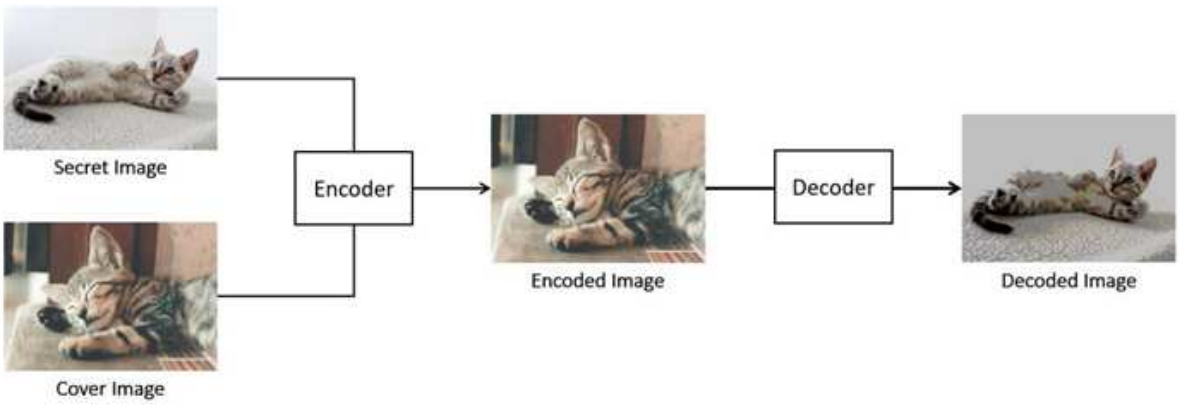

Figure 2: Work Flow

There are number methods to perform this in Python, but for simplicity we will use the easiest method, using the shift operators, extracting msb from the embedding image and placing it in the lsb of the image used as cover.

There could be an arguement the encoded image created in the encoding process is not exactly the same as the original image, but it is a good approximation (remember, we lost color channel information in the process), but at the naked eye viewers cannot tell there is a secret image hidden in the same image.

The decoding process extract now the hidden image from the encoded image, the process is kind of the same but in the opposite manner, as it is known the most significant bytes of the secret image are embedded in the less significant bytes of the encoded image, and then the lsb is just completed with zeroes.

F. Results and Discussion

The Image to Image Encoder takes the secret and cover images as input. We can specify the names of the images in the code section. After running the Encoding file, the encoded image file is created in the parent directory. When running the decoding part, the decoded image also saved in this directory.

This tool is very efficient in achieving the aim of the project, that is to conceal the secret image inside the cover image without any traces to the human eyes. A third person will not be able to find any change to the cover image. Even though there are some minor flaws, we can achieve maximum result if we take care of some guidelines while using this tool.

The image just be decoded/unhidden should be with the same number of significant bits that were used to hide the image. Otherwise, the data may contain more information than originally encoded.

Both images must be the same size or the image being hidden must be smaller. Otherwise all of the pixels won't fit if the image you're hiding Is bigger than the image used to hide.

When decoding there will be some loss of colors here and there in the decoded image but considering this a slight loss it can be neglected.

Figure 3: Secret Image

Figure 4: Cover Image

Figure 5: Encoded Image

Figure 6: Decoded Image

CONCLUSION

Now this project is developed in its very basic form. The future work is to prevent or reduce the loss of colors while decoding by improving the compression ratio of the embedded image. This will add more secrecy and security to the data storage and transfer processes. Also using this technique, we can work on hiding scannable codes like barcodes or QR codes inside images so that instead of decoding the hidden image, the encoded images can be scanned to read/view the concealed image directly from the cover image using specially software installed cameras or scanners. All these future enhancements can open doors to various possibilities and opportunities in the data security field.

There's a vast range of fields where this method or process can be used for the secure transfer or communication of data, in this case images. Also, in view of the flaws in the techniques used currently for data security, this method have a very good scope in the respective fields. Even though this method also have its own limitations, considering the advantages of this method, that all can be neglected. In future we might see more situations and fields where this method is implemented for secure data storage and transfer.

ACKNOWLEDGEMENT

I should convey my real tendency and obligation to Dr M N Nachappa and Asst. Prof: Dr Ganesh D and undertaking facilitators for their effective steerage and consistent inspirations all through my assessment work. Their ideal bearing, absolute co-action and second discernment have made my work gainful.

REFERENCES

[1] X. Zhou, W. Gong, W. Fu and L. Jin, "An improved method for LSB based color image steganography combined with cryptography," 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), 2016, pp. 1-4, doi: 10.1109/ICIS.2016.7550955.

[2] Aung Myint Aye "LSB Based Image Steganography for Information Security System" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-1, December 2018, pp.394-400

[3] Jiang, Nan & Zhao, Na & Wang, Luo. (2015). LSB Based Quantum Image Steganography Algorithm. International Journal of Theoretical Physics. 55. 10.1007/s10773-015-2640-0.

[4] J. V. Karthik and B. V. Reddy, "Authentication of secret information in image stenography," International Journal of Computer Science and Network Security (IJCSNS), vol. 14, no. 6, p. 58, 2014.

[5] Hassan, Fatuma Saeid and A. Gutub. "Novel embedding secrecy within images utilizing an improved interpolation-based reversible data hiding scheme." Journal of King Saud University - Computer and Information Sciences (2020): n. pag.

[6] Bin Li et al., "A Survey on Image Steganography and Steganalysis", Journal of Info. Hiding and Multimedia Signal Processing, ISSN 2073-4212, Vol-2, No-2, pp142-172, Apr 21011.

[7] Saleh, Mohammed. (2018). Image Steganography Techniques - A Review Paper. IJARCCE. 7. 52-58. 10.17148/IJARCCE.2018.7910

[8] J. K. Saini and H. K. Verma, "A hybrid approach for image security by combining encryption and steganography," in Image Information Processing (ICIIP), 2013 IEEE Second International Conference on. IEEE, 2013, pp. 607–611.

[9] A. Cheddad et al.: "Digital image Steganography: Survey and analysis of current methods", Signal Processing, Elsevier, 90(2010) 727-752.

[10] Neil F. Johnson: "Exploring Steganography: Seeing the Unseen", George Mason University, IEEE Computer, pp. 26-34, Feb 1998.

[11] S. Kurane, H. Harke, and S. Kulkarni, "TEXT AND AUDIO DATA HIDING USING LSB AND DCT A REVIEW APPROACH," Natl. Conf. "Internet Things Towar. a Smart Futur. "Recent Trends Electron. Commun., 2016.

[12] Neeta, Deshpande & Kamalapur, Snehal & Jacobs, Daisy. (2007). Implementation of LSB Steganography and Its Evaluation for Various Bits. 173 - 178. 10.1109/ICDIM.2007.369349.

[13] A. E. Mustafa, A. M. F. Elgamal, M. E. Elalmi, and A. Bd, "A Proposed Algorithm For Steganography In Digital Image Based on Least Significant Bit," Res. J. Specif. Educ., no. 21, 2011.

[14] Viral Kishorbhai Patel, 2021, A Review Paper on Cryptography, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 10, Issue 02 (February 2021)

[15] A. Singh and S. Malik, "Securing data by using cryptography with steganography," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 5, 2013.